An Intuitionistic Linear Logical Semantics of SAND Attack Trees

Harley Eades III

Computer Science
Augusta University
harley.eades@gmail.com

Abstract. TODO

1 Introduction

2 A Quaternary Semantics for SAND Attack Trees

Kordy et al. [4] gave a very elegant and simple semantics of attack-defense trees in boolean algebras. Unfortunately, while their semantics is elegant it does not capture the resource aspect of attack trees, it allows contraction, and it does not provide a means to model sequential conjunction. In this section we give a semantics of attack trees in the spirit of Kordy et al.'s using a four valued logic.

The propositional variables of our quaternary logic, denoted by A, B, C, and D, range over the set $\mathsf{4} = \{0, \frac{1}{4}, \frac{1}{2}, 1\}$. We think of 0 and 1 as we usually do in boolean algebras, but we think of $\frac{1}{4}$ and $\frac{1}{2}$ as intermediate values that can be used to break various structural rules. In particular we will use these values to prevent exchange for sequential conjunction from holding, and contraction from holding for parallel and sequential conjunction.

Definition 1. *The logical connectives of our four valued logic are defined as follows:*

Parallel and Sequential Conjunction:

$A \odot_4 B = 1,$
where neither A nor B are 0
$A \odot_4 B = 0,$ *otherwise*

$A \rhd_4 B = 1,$
where $A \in \{\frac{1}{2}, 1\}$ and $B \neq 0$
$\frac{1}{4} \rhd_4 B = \frac{1}{4},$ *where $B \neq 0$*
$A \rhd_4 B = 0,$ *otherwise*

Choice: $A \sqcup_4 B = \mathsf{max}(A, B)$

These definitions are carefully crafted to satisfy the necessary properties to model attack trees. Comparing these definitions with Kordy et al.'s [4] work we can see that choice is defined similarly, but parallel conjunction is not a product – ordinary conjunction – but rather a linear tensor product, and sequential conjunction is not actually definable in a boolean algebra, and hence, makes heavy use of the intermediate values to insure that neither exchange nor contraction hold.

We use the usual notion of equivalence between propositions, that is, propositions ϕ and ψ are considered equivalent, denoted by $\phi \equiv \psi$, if and only if they have the same truth tables. In order to model attack trees the previously defined logical connectives must satisfy the appropriate equivalences corresponding to the equations between attack trees. These equivalences are all proven by the following result.

Lemma 1 (Properties of the Attack Tree Operators in the Quaternary Semantics).

(Symmetry) For any A and B, $A \bullet B \equiv B \bullet A$, for $\bullet \in \{\odot_4, \sqcup_4\}$.

(Symmetry for Sequential Conjunction) It is not the case that, for any A and B, $A \rhd_4 B \equiv B \rhd_4 A$.

(Associativity) For any A, B, and C, $(A \bullet B) \bullet C \equiv A \bullet (B \bullet C)$, for $\bullet \in \{\odot_4, \rhd_4, \sqcup_4\}$.

(Contraction for Parallel and Sequential Conjunction) It is not the case that for any A, $A \bullet A \equiv A$, for $\bullet \in \{\odot_4, \rhd_4\}$.

(Contraction for Choice) For any A, $A \sqcup_4 A \equiv_4 A$

(Left Distributive Law) For any A, B, and C, $A \bullet (B \sqcup_4 C) \equiv (A \bullet B) \sqcup_4 (A \bullet C)$, for $\bullet \in \{\odot_4, \rhd_4\}$.

(Right Distributive Law) For any A, B, and C, $(A \sqcup_4 B) \bullet C \equiv (A \bullet C) \sqcup_4 (B \bullet C)$, for $\bullet \in \{\odot_4, \rhd_4\}$.

Proof. Symmetry, associativity, contraction for choice, and the distributive laws for each operator hold by simply comparing truth tables. As for contraction for parallel conjunction, suppose $A = \frac{1}{4}$. Then by definition $A \odot_4 A = 1$, but $\frac{1}{4}$ is not 1. Contraction for sequential conjunction also fails, suppose $A = \frac{1}{2}$. Then by definition $A \rhd_4 A = 1$, but $\frac{1}{2}$ is not 1. Similarly, symmetry fails for sequential conjunction. Suppose $A = \frac{1}{4}$ and $B = \frac{1}{2}$. Then $A \rhd_4 B = \frac{1}{4}$, but $B \rhd_4 A = 1$.

At this point it is quite easy to model attack trees as formulas. The following defines their interpretation.

Definition 2. *Suppose $\mathbb{B}$ is some set of base attacks, and $\nu : \mathbb{B} \longrightarrow \mathsf{PVar}$ is an assignment of base attacks to propositional variables. Then we define the interpretation of* ATerms *to propositions as follows:*

$$\begin{array}{lcllcl}
\llbracket \mathbf{b} \in \mathbb{B} \rrbracket & = & \nu(\mathbf{b}) & \llbracket \mathsf{SAND}\, T_1\, T_2 \rrbracket & = & \llbracket T_1 \rrbracket \rhd_4 \llbracket T_2 \rrbracket \\
\llbracket \mathsf{AND}\, T_1\, T_2 \rrbracket & = & \llbracket T_1 \rrbracket \odot_4 \llbracket T_2 \rrbracket & \llbracket \mathsf{OR}\, T_1\, T_2 \rrbracket & = & \llbracket T_1 \rrbracket \sqcup_4 \llbracket T_2 \rrbracket
\end{array}$$

We can use this semantics to prove equivalences between attack trees.

Lemma 2 (Equivalence of Attack Trees in the Quaternary Semantics). *Suppose $\mathbb{B}$ is some set of base attacks, and $\nu : \mathbb{B} \longrightarrow \mathsf{PVar}$ is an assignment of base attacks to propositional variables. Then for any attack trees T_1 and T_2, $T_1 \approx T_2$ if and only if $\llbracket T_1 \rrbracket \equiv \llbracket T_2 \rrbracket$.*

Proof. This proof holds by induction on the form of $T_1 \approx T_2$.

This is a very simple and elegant semantics, but it also leads to a more substantial theory.

3 Lineale Semantics for SAND Attack Trees

Classical natural deduction has a semantics in boolean algebras, and so the semantics in the previous section begs the question of whether there is a natural deduction system that can be used to reason about attack trees. We answer this question in the positive, but before defining the logic we first build up a non-trivial concrete categorical model of our desired logic in dialectica spaces, but this first requires the abstraction of the quaternary semantics into a preorder semantics we call the lineale semantics of SAND attack trees. This semantics will live at the base of the dialectica space model given in the next section, but it also begins to shed light on new and interesting reasoning tools for attack trees.

We denote by $\leq_4 \colon \mathsf{4} \times \mathsf{4} \to \mathsf{4}$ the obvious preorder on $\mathsf{4}$ making $(\mathsf{4}, \leq_4)$ a preordered set (proset). It is well known that every preordered set induces a category whose objects are the elements of the carrier set, here $\mathsf{4}$, and morphisms $\mathsf{Hom}_4(a, b) = a \leq_4 b$. Composition of morphisms hold by transitivity and identities exists by reflexivity. Under this setting it is straightforward to show that for any propositions ϕ and ψ over $\mathsf{4}$ we have $\phi \equiv \psi$ if and only if $\phi \leq_4 \psi$ and $\psi \leq_4 \phi$. Thus, every result proven for the logical connectives on $\mathsf{4}$ in the previous section induce properties on morphisms in this setting.

In addition to the induced properties just mentioned we also have the following new ones which are required when lifting this semantics to dialectica spaces, but are also important when building a corresponding logic.

Lemma 3 (Functorality). *For any A, B, C, and D, if $A \leq_4 C$ and $B \leq_4 D$, then $(A \bullet B) \leq_4 (C \bullet D)$, for $\bullet \in \{\odot_4, \rhd_4, \sqcup_4\}$.*

Proof. Each part holds by case analysis over A, B, C, and D. In any cases where $(A \bullet B) \leq_4 (C \bullet D)$ does not hold, then one of the premises will also not hold.

The logic we are building up is indeed intuitionistic, but none of the operators we have introduced thus far are closed, but we can define the standard symmetric linear tensor product in $\mathsf{4}$ that is closed.

Definition 3. *The following defines the linear tensor product on $\mathsf{4}$ as well as linear implication:*

$$\begin{array}{ll}
A \otimes_4 B = \mathsf{max}(A, B), & A \multimap_4 B = 0, \textit{where } B <_4 A \\
\quad\quad \textit{where } A \textit{ nor } B \textit{ are } 0 & A \multimap_4 A = A, \textit{where } A \in \{\frac{1}{4}, \frac{1}{2}\} \\
A \otimes_4 B = 0, \textit{otherwise} & A \multimap_4 B = 1, \textit{otherwise}
\end{array}$$

The unit of the tensor product is $I_4 = \frac{1}{4}$.

The expected monoidal properties hold for the tensor product.

Lemma 4 (Tensor is Symmetric Monoidal Closed).

(Symmetry) For any A and B, $A \otimes_4 B \equiv B \otimes A$.

(Associativity) For any A, B, and C, $(A \otimes_4 B) \otimes_4 C \equiv A \otimes_4 (B \otimes_4 C)$.

(Unitors) For any A, $(A \otimes I_4) \equiv A \equiv (I_4 \otimes A)$.

(Tensor is Functorial) For any A, B, C, and D, if $A \leq_4 C$ *and* $B \leq_4 D$*, then* $(A \otimes_4 B) \leq_4 (C \otimes_4 D)$.

(Implication is Functorial) For any A, B, C, and D, if $C \leq_4 A$ *and* $B \leq_4 D$*, then* $(A \multimap_4 B) \leq_4 (C \multimap_4 D)$.

(Closure) For any A, B, and C, $(A \otimes_4 B) \leq_4 C$ *if and only if* $A \leq_4 (B \multimap_4 C)$.

Proof. The top three cases hold by simply comparing truth tables. Finally, the last three cases hold by a case analysis over A, B, C, and D. If at any time the conclusion is false, then one of the premises will also be false.

We now define lineales which depend on the notion of a monoidal proset. The definition of lineales given here is a slight generalization over the original definition given by Hyland and de Paiva – see Definition 1 of [**?**]. They base lineales on posets instead of prosets, but the formalization given here shows that anti-symmetry can be safely dropped.

Definition 4. *A **monoidal proset** is a proset,* $(L, \leq)$*, with a given symmetric monoidal structure* $(L, \circ, e)$*. That is, a set L with a given binary relation* $\leq : L \times L \to L$ *satisfying the following:*

- *(reflexivity)* $a \leq a$ *for any* $a \in L$
- *(transitivity) If* $a \leq b$ *and* $b \leq c$*, then* $a \leq c$

together with a monoidal structure $(\circ, e)$ *consisting of a binary operation, called multiplication,* $\circ : L \times L \to L$ *and a distinguished element* $e \in L$ *called the unit such that the following hold:*

- *(associativity)* $(a \circ b) \circ c = a \circ (b \circ c)$
- *(identity)* $a \circ e = a = e \circ a$
- *(symmetry)* $a \circ b = b \circ a$

Finally, the structures must be compatible, that is, if $a \leq b$*, then* $a \circ c \leq b \circ c$ *for any* $c \in L$.

Now a lineale can be seen as essentially a symmetric monoidal closed category in the category of prosets.

Definition 5. *A **lineale** is a monoidal proset,* $(L, \leq, \circ, e)$*, with a given binary operation, called implication,* $\multimap : L \times L \to L$ *such that the following hold:*

- *(relative complement)* $(a \multimap b) \circ a \leq b$
- *(adjunction) If* $a \circ y \leq b$*, then* $y \leq a \multimap b$

The set $\mathsf{2} = \{0, 1\}$ is an example of a lineale where the order is the usual one, the multiplication is boolean conjunction, and the implication is boolean implication. This example is not that interesting, because $\mathsf{2}$ is a boolean algebra. An example of a proper lineale can be given using the three element set $\mathsf{3} = \{0, \frac{1}{2}, 1\}$, but one must be careful when defining lineales, because it is possible to instead define Heyting algebras, and hence, become nonlinear.

Given the operations and properties shown for $(4, \leq_4)$ above we can easily prove that $(4, \leq_4)$ defines a lineale.

Lemma 5. *The proset,* $(4, \leq_4, \otimes_4, I_4, \multimap_4)$ *is a lineale.*

Proof. First, $(4, \leq_4, \otimes_4, I_4)$ defines a monoidal proset, because the tensor product is associative, I_4 is the identity, and symmetric by Lemma 4. We can also show that the tensor product is compatible, that is, if $A \leq_4 B$, then $(A \otimes_4 C) \leq_4 (B \otimes C)$ for any C. Suppose $A \leq_4 B$, then by reflexivity we also know that $C \leq_4 C$. Thus, by functorality, Lemma 4, we obtain our result.

Finally, we show that $(4, \leq_4, \otimes_4, I_4, \multimap_4)$ is a lineale. The adjunction property already holds by Lemma 4, thus, all that is left to show is that the relative complement holds. We know by Lemma 4 that for any A, B, and C, if $A \leq_4 (B \multimap_4 C)$, then $(A \otimes_4 B) \leq_4 C$. In addition, we know by reflexivity that $(A \multimap_4 B) \leq_4 (A \multimap_4 B)$, thus by the previous property we obtain that $((A \multimap_4 B) \otimes_4 A) \leq_4 B$.

The interpretation of attack trees into the lineale $(4, \leq_4, \otimes_4, I_4, \multimap_4)$ does not change from Definition 10, but the equivalences between attack trees, Lemma 2, can be abstracted.

Lemma 6 (Equivalence of Attack Trees in the Lineale Semantics). *Suppose* $\mathbb{B}$ *is some set of base attacks, and* $\alpha : \mathbb{B} \longrightarrow \mathsf{PVar}$ *is an assignment of base attacks to propositional variables. Then for any attack trees* T_1 *and* T_2*,* $T_1 \approx T_2$ *if and only if* $[\![T_1]\!] \leq_4 [\![T_2]\!]$ *and* $[\![T_2]\!] \leq_4 [\![T_1]\!]$.

Proof. This proof holds by induction on the form of $T_1 \approx T_2$.

This result seems basic, but has some interesting consequences.

Recall that equivalence of attack trees is defined to be the reflexive, symmetric, and transitive closure of the attack tree simplification rules given in Definition **??**. We can now interpret these rules as morphisms.

Corollary 1 (Simplifications of Attack Trees in the Lineale Semantics). *Suppose* $\mathbb{B}$ *is some set of base attacks, and* $\alpha : \mathbb{B} \longrightarrow \mathsf{PVar}$ *is an assignment of base attacks to propositional variables. Then for any attack trees* T_1 *and* T_2 *the following hold:*

i. if $T_1 \rightsquigarrow T_2$*, then* $[\![T_1]\!] \leq_4 [\![T_2]\!]$

This corollary also implies that categorical models, and equivalently by the Curry-Howard-Lambek Correspondence, logical models of attack trees can support different notions of equivalence, because equivalence of attack trees can be broken down into morphisms. In fact, in the next section we will lift the lineale semantics up into a dialectica model, but dialectica models are models of linear logic where contraction of choice will only hold up to a natural transformation and not a natural isomorphism. Thus, in order to be able to model full equivalence of attack trees the definition of equivalence will need to be modified into an equivalent one that does not require contraction to be an isomorphism.

Kordy et al. [3] showed that the attack tree simplification rules are confluent, and hence, satisfy the Church-Rosser theorem. This result can be utilized to reformulate equivalence of attack trees into the following one.

Definition 6. *Suppose T_1 and T_2 are attack trees over some set of base attacks $\mathbb{B}$. Then $T_1 \curlyvee T_2$ if and only if there exists an attack tree S, such that, $T_1 \rightsquigarrow^* S$ and $T_2 \rightsquigarrow^* S$.*

It is fairly straightforward to show the following two results.

Lemma 7 (Joinability is an Equivalence Relation). *Suppose T_1 and T_2 are attack trees over some set of base attacks $\mathbb{B}$. Then $T_1 \curlyvee T_2$ is an equivalence relation.*

Proof. Reflexivity holds by reflexivity of the underlying reduction relation, symmetry is by definition, and transitivity holds by the Church-Rosser theorem.

Lemma 8 (Equivalence of Attack Trees and Joinability). *Suppose T_1 and T_2 are attack trees over some set of base attacks $\mathbb{B}$. Then $T_1 \approx T_2$ if and only if $T_1 \curlyvee T_2$.*

Proof. The left-to-right direction holds by induction on $T_1 \approx T_2$. The opposite direction holds by showing that if $T_1 \rightsquigarrow^* T_2$, then $T_1 \approx T_2$, which holds by induction on $T_1 \rightsquigarrow^* T_2$.

Joinability of attack trees gets around having to have full contraction for choice, because it never requires one to use its inverse. In the next section we will use this result to model equivalence of attack trees in dialectica models.

Finally, the results of this section leads us to a more logical viewpoint. If we know $[\![T_1]\!] \leq_4 [\![T_2]\!]$, then by closure $I_4 \leq_4 ([\![T_1]\!] \multimap_4 [\![T_2]\!])$. Thus, two attack trees are then equivalent if and only if they are bi-conditionally related, i.e. $I_4 \leq_4 ([\![T_1]\!] \multimap_4 [\![T_2]\!])$ and $I_4 \leq_4 ([\![T_2]\!] \multimap_4 [\![T_1]\!])$. Therefore, if we are able to find a logic that is sound with respect to the semantics laid out thus far, then we can use it to reason about attack trees using linear implication.

4 Dialectica Semantics of SAND Attack Trees

In her thesis de Paiva [**?**] gave one of the first sound and complete categorical models, called dialectica categories, of full intuitionistic linear logic. Her models arose from giving a categorical definition to Gödel's Dialectica interpretation. de Paiva defines a particular class of dialectica categories called GC over a base category C, see page 41 of [**?**]. She later showed that by instantiating C to Sets, the category of sets and total functions, that one arrives at concrete instantiation of GC she called $\mathsf{Dial}_2(\mathsf{Sets})$ whose objects are called *dialectica spaces*, and then she abstracts $\mathsf{Dial}_2(\mathsf{Sets})$ into a family of concrete dialectica spaces, $\mathsf{Dial}_L(\mathsf{Sets})$, by replacing $\mathsf{2}$ with an arbitrary lineale L.

In this section we construct the dialectica category, $\mathsf{Dial}_4(\mathsf{Sets})$, and show that it is a model of attack trees. This will be done by essentially lifting each of the attack tree operators defined for the lineale semantics given in the previous section into the dialectica category. Working with dialectica categories can be very complex due to the nature of how they are constructed. In fact, they are one of the few examples of theories that are easier to work with in a proof assistant than outside of one. Thus, throughout this section we only give brief proof sketches, but the interested reader will find the complete proofs in the formalization.

We begin with the basic definition of $\mathsf{Dial}_4(\mathsf{Sets})$, and prove it is a category.

Definition 7. *The category of dialectica spaces over* $\mathsf{4}$*, denoted by* $\mathsf{Dial_4(Sets)}$*, is defined by the following data:*

- *objects, or dialectica spaces, are triples* (U, X, α) *where* U *and* X *are sets, and* $\alpha : U \to X \to \mathsf{4}$ *is a relation on* $\mathsf{4}$*.*
- *morphisms are pairs* $(f, F) : (U, X, \alpha) \to (V, Y, \beta)$ *where* $f : U \to V$ *and* $F : Y \to X$ *such that for any* $u \in U$ *and* $y \in Y$*,* $\alpha(u, F(y)) \leq_4 \beta(f(u), y)$*.*

Lemma 9. *The structure* $\mathsf{Dial_4(Sets)}$ *is a category.*

Proof. Identity morphisms are defined by $(\mathsf{id}_U, \mathsf{id}_X) : (U, X, \alpha) \to (U, X, \alpha)$, and the property on morphisms holds by reflexivity. Given two morphism $(f, F) : (U, X, \alpha) \to (V, Y, \beta)$ and $(g, G) : (V, Y, \beta) \to (W, Z, \gamma)$, then their composition is defined by $(f; g, G; F) : (U, X, \alpha) \to (W, Z, \gamma)$ whose property holds by transitivity. Proving that composition is associative and respects identities is straightforward.

Next we show that $\mathsf{Dial_4(Sets)}$ is symmetric monoidal closed. The definitions of both the tensor product and the internal hom will be defined in terms of their respective counterparts in the lineale semantics.

Definition 8. *The following defines the tensor product and the internal hom:*

(Tensor Product) Suppose $A = (U, X, \alpha)$ *and* $B = (V, Y, \beta)$*, then define* $A \otimes B = (U \times V, (V \to X) \times (U \to Y), \alpha \otimes_r \beta)$*, where* $(\alpha \otimes_r \beta)(u, v)(f, g) = (\alpha\, u\, (f v)) \otimes_4 (\beta\, v\, (g\, u))$*.*

(Internal Hom) Suppose $A = (U, X, \alpha)$ *and* $B = (V, Y, \beta)$*, then define* $A \multimap B = ((U \to V) \times (Y \to X), U \times Y, \alpha \multimap_r \beta)$*, where* $(\alpha \multimap_4 \beta)(f, g)(u, y) = (\alpha\, u\, (g\, y)) \multimap_4 (\beta\, (f\, u)\, y)$*.*

The unit of the tensor product is defined by $I = (\top, \top, (\lambda x.\lambda y.I_4))$*, where* $\top$ *is the final object in* Set*.*

The following properties hold for the previous constructions.

Lemma 10 (SMCC Properties for $\mathsf{Dial_4(Sets)}$**).**

(Functorality for Tensor) Given morphisms $f : A \longrightarrow C$ *and* $g : B \longrightarrow D$*, then there is a morphism* $f \otimes g : (A \otimes B) \longrightarrow (C \otimes D)$*.*

(Associator) There is a natural isomorphism, $\alpha_{A,B,C} : (A \otimes B) \otimes C \longrightarrow A \otimes (B \otimes C)$*.*

(Unitors) There are natural isomorphisms, $\lambda_A : (I \otimes A) \longrightarrow A$ *and* $\rho_A : (A \otimes I) \longrightarrow A$*.*

(Symmetry) There is a natural transformation, $\beta_{A,B} : (A \otimes B) \longrightarrow (B \otimes A)$ *that is involutive.*

(Functorality for the Internal Hom) Given morphism $f : C \longrightarrow A$ *and* $g : B \longrightarrow D$*, then there is a morphism* $f \multimap g : (A \multimap B) \longrightarrow (C \multimap D)$*.*

(Adjunction) There is a natural bijection:

$$\mathsf{curry} : \mathsf{Hom}_{\mathsf{Dial_4(Sets)}}(A \otimes B, C) \cong \mathsf{Hom}_{\mathsf{Dial_4(Sets)}}(A, B \multimap C).$$

Finally, the coherence diagrams for symmetric monoidal categories – which we omit to conserve space, but can be found here [?] – also hold for the natural transformations above.

Proof. These properties are not new, and their proofs follow almost exactly de Paiva's proofs from her thesis [**?**]. The complete proofs for each of the cases above, including the proofs for the symmetric monoidal coherence diagrams, can be found in the formalization.

The constructions on $\mathsf{Dial}_4(\mathsf{Sets})$ given so far are not new, but the constructions for the attack tree operators for parallel conjunction, sequential conjunction, and choice are new to dialectica categories, but it turns out that the definition of choice we give here has been previously used in a different categorical construction called the category of Chu spaces.

Definition 9. *The attack tree operators are defined in* $\mathsf{Dial}_4(\mathsf{Sets})$ *as follows:*

(Parallel Conjunction) Suppose $A = (U, X, \alpha)$ *and* $B = (V, Y, \beta)$*, then* $A \odot B = (U \times V, X \times Y, \alpha \odot_r \beta)$*, where* $(\alpha \odot_r \beta)(u, v)(x, y) = (\alpha\, u\, x) \odot_4 (\beta\, v\, y)$*.*

(Sequential Conjunction) $A = (U, X, \alpha)$ *and* $B = (V, Y, \beta)$*, then* $A \rhd B = (U \times V, X \times Y, \alpha \rhd_r \beta)$*, where* $(\alpha \rhd_r \beta)(u, v)(x, y) = (\alpha\, u\, x) \rhd_4 (\beta\, v\, y)$*.*

(Choice) $A = (U, X, \alpha)$ *and* $B = (V, Y, \beta)$*, then* $A \sqcup B = (U + V, X + Y, \alpha \sqcup_r \beta)$*, where*

$$\begin{array}{l}
(\alpha \odot_r \beta)\, a\, b = \alpha\, a\, b, \textit{when } a \in U \textit{ and } b \in X\\
(\alpha \odot_r \beta)\, a\, b = \beta\, a\, b, \textit{when } a \in V \textit{ and } b \in Y\\
(\alpha \odot_r \beta)\, a\, b = 0, \textit{otherwise}
\end{array}$$

The definitions of parallel and sequential conjunction are quite literally the lifting of their lineale counterparts. The parallel and sequential operators on $(4, \leq_4, \otimes_4, I_4, \multimap_4)$, $\odot_4$ and $\rhd_4$, restrict the cartesian product to the required properties for attack trees. Now choice must be carefully constructed so that we may prove the required distributive laws and contraction.

Given a dialectica space, (U, X, α), we can consider U as a set of actions and X as a set of states. Then given an action, $a \in U$, and a state, $q \in X$, $\alpha\, a\, q$, indicates whether action a will execute in state q. This implies that an action a and a state q of $A \sqcup B$, for $A = (U, X, \alpha)$ and $B = (V, Y, \beta)$, are either an action of A or an action of B, and a state of A or a state of B. Then an action, a, of $A \sqcup B$ will execute in state q of $A \sqcup B$ if they are both from A or both from B. Thus, the definition of choice very much fits the semantics of a choice operator. It is well known that the cartesian product distributes over the disjoint union in Sets, and because of the definitions of parallel and sequential conjunction, and choice, these properties lift up into $\mathsf{Dial}_4(\mathsf{Sets})$.

It turns out that the definition of choice given here is not new at all, but first appeared as the choice operator used for modeling concurrency in Chu spaces due to Gupta and Pratt [2]. Chu spaces are the concrete objects of Chu categories just like dialectica spaces are the concrete objects of dialectica categories. In fact, Chu categories and dialectica categories are cousins [1]. Chu and dialectica categories have exactly the same objects, but the condition on morphisms is slightly different, for Chu categories the condition uses equality instead of the preorder. The impact of this is significant, Chu spaces are a model of classical linear logic, while dialectica categories are a model of intuitionistic linear logic. At this point one natural question to ask is since choice is an object of both Chu and dialectica categories does it bring any additional structural rules with it? In fact, it does, we are able to show that there is a natural transformation, $\mathsf{contract}^{\sqcup} : (A \sqcup A) \longrightarrow A$, in $\mathsf{Dial}_4(\mathsf{Sets})$, but this is exactly what we want, because choice in attack trees contracts, however, this is not an isomorphism which sets the dialectica semantics of attack trees apart from the quaternary and lineale semantics. Keep in mind that no other operator presented here satisfies contraction.

The following gives all of the properties that hold for the attack tree operators in $\mathsf{Dial}_4(\mathsf{Sets})$.

Lemma 11 (Properties of the Attack Tree Operators in $\mathsf{Dial}_4(\mathsf{Sets})$).

> *(Functorality) Given morphisms $f : A \longrightarrow C$ and $g : B \longrightarrow D$, then there is a morphism $f \bullet g : (A \bullet B) \longrightarrow (C \bullet D)$, for $\bullet \in \{\odot, \rhd, \sqcup\}$.*
>
> *(Associativity) There is a natural isomorphism, $\alpha^{\bullet}_{A,B,C} : (A \bullet B) \bullet C \longrightarrow A \bullet (B \bullet C)$, for $\bullet \in \{\odot, \rhd, \sqcup\}$.*
>
> *(Symmetry) There is a natural transformation, $\beta^{\bullet}_{A,B} : (A \bullet B) \longrightarrow (B \bullet A)$ that is involutive, for $\bullet \in \{\odot, \rhd, \sqcup\}$.*
>
> *(Choice is Contractive) There is a natural transformation, $\mathsf{contract}^{\sqcup} : (A \sqcup A) \longrightarrow A$.*
>
> *(Left Distributive Laws) There is a natural isomorphism, $distl^{\bullet} : A \bullet (B \sqcup C) \longrightarrow (A \bullet B) \sqcup (A \bullet C)$, for $\bullet \in \{\odot, \rhd\}$.*
>
> *(Right Distributive Laws) There is a natural isomorphism, $distr^{\bullet} : (A \sqcup B) \bullet C \longrightarrow (A \bullet C) \sqcup (B \bullet C)$, for $\bullet \in \{\odot, \rhd\}$.*

At this point we can interpret attack trees into $\mathsf{Dial}_4(\mathsf{Sets})$, but because $\mathsf{contract}^{\sqcup}$ is only a natural transformation and not an isomorphism we have to rethink proving equivalences between attack trees.

Definition 10. *Suppose $\mathbb{B}$ is some set of base attacks, and $\nu : \mathbb{B} \longrightarrow \mathsf{Obj}(\mathsf{Dial}_4(\mathsf{Sets}))$ is an assignment of base attacks to dialectica spaces. Then we define the interpretation of* ATerms *to objects of* $\mathsf{Dial}_4(\mathsf{Sets})$ *as follows:*

$$\begin{array}{rclcrcl}
[\![\mathbf{b} \in \mathbb{B}]\!] & = & \nu(\mathbf{b}) & \quad & [\![\mathsf{OR}\, T_1\, T_2]\!] & = & [\![T_1]\!] \sqcup [\![T_2]\!] \\
[\![\mathsf{AND}\, T_1\, T_2]\!] & = & [\![T_1]\!] \odot [\![T_2]\!] & \quad & [\![\mathsf{SAND}\, T_1\, T_2]\!] & = & [\![T_1]\!] \rhd [\![T_2]\!]
\end{array}$$

Let $T_1 \simeq T_2$ be $T_1 \approx T_2$ without contraction for choice. Then we have the following result.

Lemma 12 (Non-contractive Equivalence of Attack Trees in the Dialectica Semantics). *Suppose $\mathbb{B}$ is some set of base attacks, and $\nu : \mathbb{B} \longrightarrow \mathsf{Obj}(\mathsf{Dial}_4(\mathsf{Sets}))$ is an assignment of base attacks to dialectica spaces. Then for any attack trees T_1 and T_2, $T_1 \simeq T_2$ if and only if there is an isomorphism $m : [\![T_1]\!] \longrightarrow [\![T_2]\!]$ in* $\mathsf{Dial}_4(\mathsf{Sets})$.

Proof. This proof holds by induction on the form of $T_1 \simeq T_2$.

Modeling full equivalence of attack trees, $T_1 \approx T_2$, requires contraction for choice, but by redefining the equivalence operator we can regain full equivalence in the model. Denote by S_i the sublanguage of attack trees with no occurrences of $\mathsf{OR}\,T\,T$ for any attack tree T. Now denote by $T_1 \rightsquigarrow_{©} T_2$ the subrewrite system of $T_1 \rightsquigarrow T_2$ consisting only of $\mathsf{OR}\,T\,T \rightsquigarrow T$ and the obvious congruence rules. This rewrite system is terminating and confluent, because it is a subsystem of $T_1 \rightsquigarrow T_2$ which was shown to be terminating and confluent by Kordy et al. [3]. We now arrive at the following result.

Lemma 13. *Suppose T_1 and T_2 are two attack trees. Then $T_1 \approx T_2$ if and only if there are attack trees S_1 and S_2 such that $T_1 \rightsquigarrow^*_{©} S_1$, $T_2 \rightsquigarrow^*_{©} S_2$, and $S_1 \simeq S_2$.*

Proof. ($\Rightarrow$) Suppose T_1 and T_2 are two attack trees such that $T_1 \approx T_2$. Since $\rightsquigarrow^*_{©}$ is a subsystem of $\approx$, then if T_1 or T_2 has a subtree of the form $\mathsf{OR}\,T\,T$ for some T, then there are attack trees S_1 and S_2 such that $T_1 \approx S_1$ and $T_2 \approx S_2$ using only the rules for contraction and congruences, but this implies that $T_1 \rightsquigarrow^*_{©} S_1$ and $T_2 \rightsquigarrow^*_{©} S_2$. Furthermore, since $T_1 \approx T_2$, then it must be the case that $S_1 \simeq S_2$, because S_1 and S_2 only differ from T_1 and T_2 by contractions.
($\Leftarrow$) Suppose there are attack trees T_1, T_2, S_1 and S_2 such that $T_1 \rightsquigarrow^*_{©} S_1$, $T_2 \rightsquigarrow^*_{©} S_2$, and $S_1 \simeq S_2$. Clearly, $T_1 \approx S_1$, $T_2 \approx S_2$, and $S_1 \approx S_2$, because $\approx$ subsumes both $\rightsquigarrow^*_{©}$ and $\simeq$. Therefore, by transitivity $T_1 \approx T_2$.

We now use the previous result to model full equivalence of attack trees including contraction.

Theorem 1 (Equivalence of Attack Trees in the Dialectica Semantics). *Suppose $\mathbb{B}$ is some set of base attacks, and $v : \mathbb{B} \longrightarrow \mathsf{Obj}(\mathsf{Dial}_4(\mathsf{Sets}))$ is an assignment of base attacks to dialectica spaces. Then for any attack trees T_1 and T_2, if there are attack trees S_1 and S_2 such that $T_1 \rightsquigarrow^*_{©} S_1$, $T_2 \rightsquigarrow^*_{©} S_2$, and $S_1 \simeq S_2$, then there are natural transformations $s_1 : [\![T_1]\!] \longrightarrow [\![S_1]\!]$, $s_2 : [\![T_1]\!] \longrightarrow [\![S_2]\!]$, and a natural isomorphism $m : [\![S_1]\!] \longrightarrow [\![S_2]\!]$.*

References

1. Valeria de Paiva. Dialectica and chu constructions: Cousins? *Theory and Applications of Categories*, 17(7):127–152, 2006.
2. Vineet Gupta. *Chu Spaces: a Model of Concurrency*. PhD thesis, Stanford University, 1994.
3. Barbara Kordy, Piotr Kordy, and Yoann van den Boom. *SPTool – Equivalence Checker for* SAND *Attack Trees*, pages 105–113. Springer International Publishing, Cham, 2017.
4. Barbara Kordy, Marc Pouly, and Patrick Schweitzer. Computational aspects of attack–defense trees. In Pascal Bouvry, MieczysławA. Kłopotek, Franck Leprévost, Małgorzata Marciniak, Agnieszka Mykowiecka, and Henryk Rybiński, editors, *Security and Intelligent Information Systems*, volume 7053 of *Lecture Notes in Computer Science*, pages 103–116. Springer Berlin Heidelberg, 2012.

Appendix